

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF HAWAII

UNITED STATES OF AMERICA,

Plaintiff,

vs.

LINDSEY KINNEY,

Defendant.

Case No. 22-cr-31-DKW

**ORDER DENYING DEFENDANT
LINDSEY KINNEY’S MOTION TO
SUPPRESS EVIDENCE OBTAINED
PURSUANT TO APRIL 12, 2022
SEARCH WARRANT**

Defendant Lindsey Kinney moves to suppress evidence obtained pursuant to a search warrant, alleging that the warrant lacked particularity and was overbroad. *See* Dkt. No. 53. The evidence Kinney wishes to suppress includes various contents from Kinney’s smart phone—such as messages and chat conversations, web browsing history, photos, and videos—along with forensic evidence pertaining to the use of the phone. Because Kinney’s assertions depend, in large part, on a mischaracterization of the warrant, the motion is DENIED.

LEGAL STANDARD

The Fourth Amendment to the U.S. Constitution guarantees “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures” This provision generally prohibits warrantless searches. *See Coolidge v. New Hampshire*, 403 U.S. 443, 444 (1971).

The Fourth Amendment also provides that “no Warrants shall issue, but upon probable cause . . . particularly describing the place to be searched, and the persons or things to be seized.” The Ninth Circuit construes this provision as mandating a level of “specificity” in a warrant application, which includes “two aspects: particularity and breadth.” *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702 (9th Cir. 2009) (citation omitted).

I. Particularity

In order to meet the “particularity” requirement, a warrant “must clearly state what is sought”; it “must make clear to the executing officer exactly what it is that he or she is authorized to search for and seize.” *See SDI*, 568 F.3d at 702. That said, a warrant merely needs to be “reasonably specific, rather than elaborately detailed.” *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006). Indeed, “warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible.” *Id.* “[T]he level of detail necessary in a warrant is related to the particular circumstances and the nature of the evidence sought.” *Id.* Moreover, in the Ninth Circuit, the language in a supporting affidavit is considered incorporated into the warrant itself. *See SDI*, 568 F.3d at 701 (citing *United States v. Vesikuru*, 314 F.3d 1116, 1121 (9th Cir. 2002)).

II. Overbreadth

The second aspect of “specificity” mandates that the warrant avoid overbreadth. *See id.* at 702. This mandate requires that the scope of the search warrant be “limit[ed] . . . by the probable cause on which the warrant is based.” *United States v. Fries*, 781 F.3d 1137, 1151 (9th Cir. 2015). In other words, to avoid overbreadth, the warrant must limit the Government’s search, inspection, and/or seizure to the specific places and things necessary to confirm or dispel the suspicion that gave rise to the probable cause on which the warrant is based. As the Ninth Circuit has put it:

A warrant must not only give clear instructions to a search team, it must also give legal, that is, not overbroad, instructions. Under the Fourth Amendment, this means that there must be probable cause to seize the particular thing[s] named in the warrant. . . . The number of files that [may] be scrutinized . . . is not determinative. The search and seizure of large quantities of material is justified if the material is within the scope of the probable cause underlying the warrant.

SDI, 568 F.3d at 702–03 (internal quotation marks and citation omitted).

RELEVANT FACTUAL BACKGROUND

Kinney is charged with making multiple interstate threats to injure multiple other persons, in violation of 18 U.S.C. § 875(c), specifically by posting on Instagram January and March 2022 messages to injure and/or kill several alleged victims by “beheading” and/or “other means.” *See* Superseding Indictment, Dkt. No. 47.

On April 12, 2022, the United States submitted an application for a warrant, along with a supporting affidavit, to a Magistrate Judge. The warrant sought authority to locate and seize:

All evidence of violations of 18 U.S.C. § 875(c) by Lindsey KINNEY or other[] yet to be identified individuals, including:

1. Digital devices such as cell phones, computers, tablets, and digital storage media and devices (such as hard drives, thumb drives, DVD's, CDs, and SD cards), including the cell phone assigned call number [(XXX) XXX]-3006, all of which pursuant to this warrant may be searched for evidence, fruits and instrumentalities of violations of 18 U.S.C. § 875(c) by Lindsey KINNEY, and evidence of how the digital device was used, the purpose of its use, who used it, and when; and
2. Documents and identification which may be used to positively identify the carrier of said documents and devices.

See Dkt. No. 53 at 44–45. It further sought authority for the FBI to “deliver a complete copy of the seized or copied electronically stored information to the custody and control of attorneys for the [G]overnment and their support staff for their independent review.” *Id.* at 46.

The supporting affidavit, signed by FBI Special Agent Wyatt Tackett, detailed facts constituting probable cause to believe (i) that Kinney had made the violent threats on Instagram in violation of 18 U.S.C. § 875(c); (ii) that an unidentified person had joined in one of the threats; and (iii) that evidence of the commission of the violations would be found on Kinney’s cell phone. *Id.* at 24–

43. More specifically, the affiant-agent swore to in-depth, detailed descriptions of the following events:

- A January 5, 2022 encounter between an associate of Kinney's and one of the alleged victims in Count 1. *Id.* at 26–28.
- A Facebook live stream video posted by the associate involved in the January 5, 2022 encounter, in which the associate streamed footage of the January 5, 2022 event and subsequently asked his followers to identify the names and residences of some of the individuals visible in the live stream, including the alleged victim involved in that encounter. *Id.* at 28.
- Kinney's January 17, 2022 Instagram posts, which constitute the alleged violations of § 875(c) in Count 1. *Id.* at 29–35.
- Additional events involving the alleged victims of the January 17, 2022 posts, in the aftermath of those posts, including the alleged victims' communications to the FBI about those posts. *Id.*
- Kinney's March 28, 2022 Instagram posts, which constitute the alleged violations of § 875(c) in Count 2. *Id.* at 36–37.

The affiant-agent also stated that the warrant application was seeking permission “to locate not only electronically stored information that might serve as direct evidence of the crimes described in the warrant application, but also forensic evidence that establishes how the digital devices were used, the purpose of the use, the identities of the users, and the timing of the use.” *Id.* at 38. He then provided the basis for his belief that such evidence, as it related to the charged crimes, would be present on Kinney's iPhone. *Id.* at 38–40. With regard to the scope of the authority requested, the affiant-agent explained:

[T]he warrant I am applying for would permit the examination of digital devices consistent with the warrant. The examination may require authorities to employ techniques in the field or in a laboratory environment equipped with forensic tools, including but not limited to computer-assisted scans of the entire digital device, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

Id. at 40.

The Magistrate Judge approved the warrant, which resulted in the seizure of Kinney’s iPhone by federal agents. *See* Dkt. No. 53 at 2. According to defense counsel, the agents copied “all the electronic data from the cell phone” using a program called Cellebrite and preserved it in a file. Dkt. No. 53-1 ¶ 4.

RELEVANT PROCEDURAL BACKGROUND AND ARGUMENTS

On October 31, 2022, Kinney filed a motion to suppress all iPhone evidence obtained pursuant to the April 12, 2022 search warrant, claiming that the warrant was insufficiently specific, both in terms of particularity and breadth. Dkt. No. 53.

With regard to particularity, Kinney argues that the warrant impermissibly allowed the Government to search every piece of data on his iPhone, without limitation. *Id.* at 7–10 (“[T]he warrant effectively authorized the police to freely review every message, email, snapchat, communication, bank account record, credit card statement, GPS location, accessed website, and photograph located on the device.”). Moreover, Kinney asserts that the Government, in fact, followed through on such authority when it executed the warrant, by copying, preserving,

and inspecting every piece of data on Kinney’s iPhone, without apparent limitation. To demonstrate the scope of the content that was in fact seized and searched, defense counsel explains:

Discovery produced by the Government herein has included a full Cellebrite file as well as a scoped Cellebrite file containing electronic data from the cell phone seized on April 13, 2022. Per the Government’s representations, my understanding is that the full Cellebrite file includes all the electronic data from the cell phone and the scoped file includes a subset of that data. . . .

Cellebrite uses tabs to organize electronic data copied from a smart phone. In this case, the tabs in Cellebrite containing data included Chats (containing all the messaging sent to and from the phone), Web History (documenting all of Mr. Kinney’s web browsing and searches), Images (including every photo taken, received, and/or viewed and saved on the phone), Videos (including videos created, received, and viewed on the phone), and Timeline (compiling all of the above and more in chronological order).

Among other things, the items tagged and reviewed from the seized iPhone also revealed Mr. Kinney’s Web activities (he reviewed the Honolulu StarBulletin Hawai‘i News, stories about official corruption, and Honolulu Police Department policies), review of all sorts of conspiracy theories (involving official corruption, COVID, human trafficking, and many others), his shopping habits (searching leis, koa wood products, pendants, a book titled “A Timeline to Tyranny”), and an apparent interest in numerology.

Dkt. No. 53-1 ¶¶ 4–6. Kinney contends that the warrant should have authorized the search of narrower categories of data, *e.g.*, “evidence of whether the device was used to post the alleged threats or in connection with the alleged threats,” or “evidence within a reasonable time period before and after th[e] alleged threats were made.” Dkt. No. 53 at 9.

With regard to breadth, Kinney claims that, under Ninth Circuit precedent, when a judge issues a warrant authorizing the search of a computer or its electronic equivalent, like an iPhone, certain safeguards are called for to ensure that the Government is not authorized to search every bit of the vast amount of data potentially present on the device. Kinney contends that such safeguards were not present here.

In support, Kinney first cites to *United States v. Tamura* for the proposition that, in a case like this one, *some* additional safeguards *must* be imposed by the judicial officer issuing the warrant. *See* Dkt. No. 53 at 12. *Tamura* held that, in cases that necessitate the seizure of large amounts of documents, some of which are not likely to be within the scope of probable cause on which the warrant is based, the warrants must include *some* safeguards, though it did not articulate exactly what those safeguards ought to be. 694 F.2d 591, 595 (9th Cir. 1982) (reasoning that “the wholesale seizure for later detailed examination of records not described in a warrant” is not allowable because it is equivalent to “the kind of investigatory dragnet that the fourth amendment was designed to prevent”). *Tamura* allowed that “all items in a set of files may be inspected during a search, *provided that* sufficiently specific guidelines for identifying the documents sought are provided in the search warrant and are followed by the officers conducting the search.” *Id.* (emphasis added). That court went on to advise, “In the

comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, we suggest that the Government and law enforcement officials generally can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search” *Id.* at 595–96. Kinney opines that this warrant contained *no* safeguards of the sort required by *Tamura*.

Kinney also relies on *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010), a case involving the search of a digital device. There, the Ninth Circuit *en banc* recognized “the reality that over-seizing is an inherent part of the electronic search process” and suggested that, under *Tamura*, a warrant authorizing such an electronic search “calls for greater vigilance on the part of judicial officers in striking the right balance” between the Government’s need to enforce the law and the individual’s constitutional rights. *Id.* In a concurring opinion, Judge Kozinski offered several specific, but non-binding, safeguards designed to help judicial officers strike the requisite balance:

I write separately because these issues are important and likely often to arise again. It would therefore be useful to provide guidance about how to deal with searches of electronically stored data in the future so that the public, the [G]overnment and the courts of our circuit can be confident such searches and seizures are conducted lawfully. The guidance below offers the [G]overnment a safe harbor, while protecting the people’s right to privacy and property in their papers and effects. District and magistrate judges must exercise their independent judgment in every case, but heeding this guidance will significantly increase the likelihood that the searches and seizures of

electronic storage that they authorize will be deemed reasonable and lawful.

When the [G]overnment wishes to obtain a warrant to examine a computer hard drive or electronic storage medium to search for certain incriminating files . . . , magistrate judges should insist that the [G]overnment forswear reliance on the plain view doctrine . . . [or] any similar doctrine that would allow retention of data obtained only because the [G]overnment was required to segregate seizable from non-seizable data. This will ensure that future searches of electronic records do not “make a mockery of *Tamura*”—indeed, the Fourth Amendment—by turning all warrants for digital data into general warrants. If the [G]overnment doesn’t consent to such a waiver, the magistrate judge should order that the seizable and non-seizable data be separated by an independent third party under the supervision of the court, or deny the warrant altogether. . . .

The process of sorting, segregating, decoding and otherwise separating seizable data (as defined by the warrant) from all other data should also be designed to achieve that purpose and that purpose only. Thus, if the [G]overnment is allowed to seize information pertaining to ten names, the search protocol should be designed to discover data pertaining to those names only, not to others, and not those pertaining to other illegality. For example, the government has sophisticated hashing tools at its disposal that allow the identification of well-known illegal files (such as child pornography) without actually opening the files themselves. . . .

To that end, the warrant application should normally include, or the issuing judicial officer should insert, a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown. The procedure might involve, as in this case, a requirement that the segregation be done by specially trained computer personnel who are not involved in the investigation. In that case, it should be made clear that *only* those personnel may examine and segregate the data. . . .

Once the data has been segregated (and, if necessary, redacted), the [G]overnment agents involved in the investigation should be allowed to examine only the information covered by the terms of the warrant.

Absent further judicial authorization, any remaining copies should be destroyed or, at least so long as they may be lawfully possessed by the party from whom they were seized, returned along with the actual physical medium that may have been seized (such as a hard drive or computer). . . .

Also, within a time specified in the warrant, which should be as soon as practicable, the [G]overnment should provide the issuing officer with a return disclosing precisely what it has obtained as a consequence of the search, and what it has returned to the party from whom it was seized. The return should include a sworn certificate that the [G]overnment has destroyed or returned all copies of data that it's not entitled to keep. . . .

This guidance is hardly revolutionary. It's essentially *Tamura's* solution to the problem of necessary over-seizing of evidence. Just as *Tamura* has served as a guidepost for decades, the procedures outlined above should prove a useful tool for the future. Nothing any appellate court could say, however, would substitute for the sound judgment that magistrate judges must, and I am confident will, exercise in striking this delicate balance.

See id. at 1178–80 (Kozinski, C.J., concurring with Kleinfeld, J., Fletcher, J., Paez, J., and Smith, J.).

On November 15, 2022, the Government opposed Kinney's motion to suppress the evidence obtained pursuant to the April 12, 2022 warrant, principally contending that Kinney had "mischaracterize[d] the scope of the warrant." Dkt. No. 59 at 1. Specifically, the Government points to the overarching language in the warrant that authorized a search for "evidence of violations of . . . § 875(c)." The Government contends that this language necessarily cabined the subsequent language authorizing the otherwise more expansive search for any "evidence of

how the digital device was used, the purpose of its use, who used it, and when.”

Id. at 6.¹ The Government further contends that this overarching, preceding language “severely limit[ed] the amount and type of data that the [G]overnment [was allowed to] seize[] from the cellphone, and by its own terms narrow[ed] the seizure of how/why/who/when data to evidence connected to § 875(c) crimes.” *Id.*

Kinney did not submit an optional Reply brief by the given deadline of November 21, 2022, or anytime thereafter. *See* Dkt. No. 54.

The Court heard oral argument on November 23, 2022. *See* Dkt. No. 79. Following both parties’ arguments, the Court orally DENIED the motion to suppress, and this written Order now follows.

DISCUSSION

The Court agrees with the Government that the search warrant here was sufficiently particular and not overbroad.

With regard to particularity, contrary to Kinney’s assertions, the warrant did not allow the Government to search the iPhone for *any* content revealing the how/why/who/when of its use. Rather, the warrant allowed the Government to search the iPhone for such evidence only insofar as it was connected to “evidence of violations of 18 U.S.C. § 875(c).” *See id.* In other words, according to the plain

¹The Court notes that, although Kinney appended the complete warrant to his motion, the omission of this important contextual language from the body of the motion constituted a glaringly incomplete version of the pertinent facts.

language of the warrant, the authority to search for the how/why/who/when evidence was a *subset* of the broader authority to search for evidence of the particular crimes for which probable cause existed. Moreover, the twenty-page affidavit, which was incorporated into the warrant itself, *see SDI Future Health*, 568 F.3d at 701, contained significant detail describing the crimes alleged and the way in which Kinney’s iPhone was connected to those crimes. When viewed in the light provided by the affidavit, the warrant “clearly state[d] what [wa]s sought” and “ma[d]e clear to the executing officer[s] exactly what it [wa]s that [they were] authorized to search for and seize.” *See id.* at 702.

In addition, to the extent that the warrant described only “generic categories of items,” it was “not necessarily invalid” because “a more precise description of the items subject to seizure” may not have been possible, and Kinney has not shown otherwise. *See Hill*, 459 F.3d at 973. The crimes with which Kinney is charged require the Government to prove, *inter alia*, Kinney’s subjective intent in making the Instagram posts in early 2022. The Government may attempt to prove that intent, in part, by referring to other posts Kinney has made in the same medium, *e.g.* on his Instagram accounts. Therefore, it may not have been possible for the Government to cabin their search for evidence pertaining to the use or content of the Instagram accounts by, for instance, referring to any particular time

frame. *See Hill*, 459 F.3d at 973 (“[T]he level of detail necessary in a warrant is related to the particular circumstances and the nature of the evidence sought.”).

With regard to breadth, the Court agrees that *Tamura* requires some additional safeguards in a case like this one, in order to protect against “the kind of investigatory dragnet that the fourth amendment was designed to prevent.” *See* 694 F.2d at 595. However, such safeguards existed here, even though the warrant lacked the *specific* permissive safeguards suggested by the concurring opinion in *Comprehensive Drug Testing*. *See* 621 F.3d at 1178–80. For example, the affidavit provided substantial detail regarding the type of data that may constitute evidence of the charged violations, along with information about the type and amount of evidence the Government was authorized to inspect. Though the number of files the warrant authorized the Government to scrutinize may have been large, that fact is not fatal to the warrant. *See SDI*, 568 F.3d at 702–03. (“The number of files that [may] be scrutinized . . . is not determinative. The search and seizure of large quantities of material is justified if the material is within the scope of the probable cause underlying the warrant.”). Furthermore, Kinney has neither argued nor established that the Government *failed to follow* that safeguard by collecting and examining evidence that exceeded the scope of the warrant. *See Tamura*, 694 F.2d at 595 (“[A]ll items in a set of files may be inspected during a search, provided that sufficiently specific guidelines for

identifying the documents sought are provided in the search warrant and are followed by the officers conducting the search.”); Dkt. No. 59 at 1 (pointing out that Kinney did “*not* . . . argue that the [G]overnment seized items beyond the scope of the warrant” or without probable cause) (emphasis in original). The warrant is not overbroad.


CONCLUSION

For the foregoing reasons, Kinney’s motion to suppress the digital evidence obtained pursuant to the April 12, 2022 search warrant, Dkt. No. 53, is DENIED.

IT IS SO ORDERED.

DATED: December 5, 2022 at Honolulu, Hawai‘i.




Derrick K. Watson
Chief United States District Judge

United States of America v. Lindsey Kinney; Cr No. 22-00031 DKW; **ORDER DENYING DEFENDANT LINDSEY KINNEY’S MOTION TO SUPPRESS EVIDENCE OBTAINED PURSUANT TO APRIL 12, 2022 SEARCH WARRANT**